Hidden Threats

Rick Dudley
Principal Technology Specialist
National Technology Team
Microsoft Corporation

Agenda

- Threatscape and General Trends
- Hidden Threats
- Open chat: Update on Microsoft

Threatscape

- Public threats: Viruses and Worms
- Private threats:
  Rootkits, Trojans, Backdoors, Spyware...

...Both classes of threats are complementary: either one may be used to effect the other

Common theme of both is compromise of maximum number of machines

Public Threats: Viruses and Worms

- Usually follow publication of exploit
- May follow release of patch
- Payload can be a private threat
- Initial infection via unpatched machines, unfiltered email, misconfiguration, or social engineering

Private Attacks

- Rootkits, Trojans, Backdoors, etc.
  - Difficult to detect, may go undetected for long periods
  - Popular in ‘stealth hosting’ schemes
  - Initial method of infection: unpatched machines, poorly configured machines, weak passwords, rogue admins

Rootkits: Why are they particularly interesting to attackers?

- They can be nearly impossible to detect
  - Code is frequently customized
- Machine can be safely left as a ‘sleeper’ until needed by the attacker

Rootkits: How are they transmitted?

- Attacker gains access to privileged account on machine
  - well-known vulnerability
  - misconfiguration
  - weak password
- Drops ‘rootkit’ files onto the machine
- May also leave a backdoor to enable attacker to regain control if the rootkit is detected

Rootkits: What can they do?

- Attacker has system-level control of the machine and can hide the presence of associated files and other telltale signs of infection *even from administrators*
- May hide themselves in system processes, and appearing to be normal machine activity
- Monitor/change activity and data on the machine, remove themselves when the desired task is complete, and remove all traces of their activity and their existence.

Tip: Cleaning Viruses and Worms

Once an attacker has has obtained administrative rights, you can no longer trust the machine, or the data on it—resist the temptation to try to clean it: **reformat the system drive, rebuild and restore data from backup.**

Rootkits: Detection

Rootkits are designed to be invisible, to report incorrect state information to the administrator

- Be suspicious if you see:
  - Degraded performance or random reboots, anything unusual
- Detection is difficult, get forensic help if you think you're compromised
- Prevention is the only real solution: manage your environment!

Rootkits: Preventive Measures

- Change and Configuration Management
  - Deploy securely configured standard images for each class of machine: app server, domain controller, web server, etc.
  - Confirm configuration regularly
- Have a plan for known vulnerabilities
  - How fast can you patch? What will you do when it's not fast enough? Who is responsible?
- Strengthen passwords

Hackers Strike Advanced Computing Networks

By Brian Krebs
washingtonpost.com Staff Writer
Tuesday, April 13, 2004; 5:40 PM

Hackers infiltrated powerful supercomputers at colleges, universities and research institutions in recent weeks, disrupting one of the nation's largest online research networks for several days and raising concerns among computer security experts that the compromised machines could be used to attack specific Web sites or parts of the Internet.

As many as 20 institutions were targeted, according to

——Cyber-Security——
- Microsoft Finds New Windows Security Flaws (The Washington Post, Apr 14, 2004)
- A Need for Greater Cybersecurity (The Washington Post, Apr 12, 2004)
- Worm Triggers Attacks on File-Trading Services (The Washington Post, Apr 10, 2004)
- More Security News

Tools for the Microsoft Platform

- Microsoft Baseline Security Analyzer
- Security Templates
- Group Policy

CHALLENGES

General Trends

- More of same, only
  - Vulnerabilities discovered more quickly
  - Faster exploits
  - More complex, more difficult to detect
- Most common method of entering the network:
  - Unpatched machines
  - Weak passwords
  - Social engineering
- Expect it to get worse

CHALLENGES

Good Assumptions

- The attacker may know the vulnerability before you do
- The attack may be too fast to detect/stop
- The attack may be silent
- The attacker may have the capability to marshal substantial resources to use against you.

Baseline Security

- Assess your environment
  - Security is based on risk assessment--you can't assess risk if you don't know what it is or what it does
- Integrate threat modeling into your business processes
- Create and distribute standard builds
- Create standard configurations for various classes of machines
- Automate enforcement and auditing
- Establish documentation as ongoing part of engineering and operations

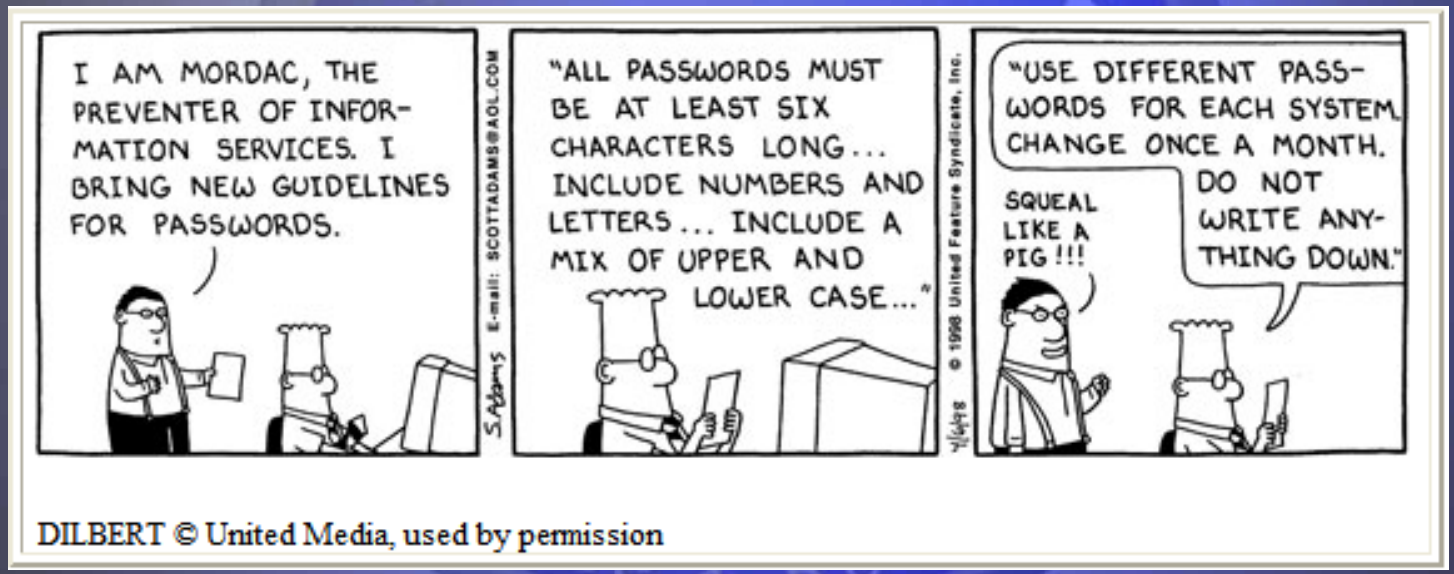
Patching

Unpatched machines represent the most common vector for both public and private attacks

- *Efficient* patching processes
  - Which machines are/are not patched
  - How long it takes to deliver patches
  - Who is responsible
- Crises
  - How do you call a crisis, and who calls it? Know everyone's role in the response.
  - Practice

CHALLENGES

Passwords according to Mordac, Preventer of Information Services



Password Management

- First of all understand that the problem is critical
- Strengthen existing password policy
- Explore strong authentication
  - 2-factor for VPN users and admins in place
- Remember that you will be attacked at the point of your weakest link: security policy must be consistent across the organization

Summary

Reactive security is a bad bet

- Protect and audit all privileged accounts
- Use the strongest authentication that you can
- Develop a defense-in-depth security strategy
- Lastly, remember that physical access to a server trumps all security!

Resources

- Gregg Keizer. Virus-Writers Using Spammer Techniques to Speed Spread, http://www.internetweek.com/security02/showArticle.jhtml?articleID=10300197
- **Results of the Distributed-Systems Intruder Tools Workshop**
-
- Pasted from <http://www.cert.org/reports/dsit_workshop-final.html>
-
- **Making a Faster Cryptanalytic Time-Memory Trade-Off**
- *Philippe Oechslin*
-
- Pasted from <http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Oech03>
-
- Cloaking Device Made for Spammers http://computercops.biz/article3536.html
- Russia and China 'behind current SPAM deluge http://www.zdnet.com.au/insight/toolkit/security/systems/0,39023913,39150051,00.htm
- Creating Stronger Passwords http://www.microsoft.com/security/articles/password.asp

Questions?